

Configurer ECMP avec IP SLA sur FTD géré par FDM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Étape 0. Préconfigurer les interfaces/objets](#)

[Étape 1. Configuration de la zone ECMP](#)

[Étape 2. Configurer des objets IP SLA](#)

[Étape 3. Configuration de routes statiques avec route track](#)

[Vérifier](#)

[Équilibrage de charge](#)

[Route perdue](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer ECMP avec IP SLA sur un FTD qui est géré par FDM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration ECMP sur Cisco Secure Firewall Threat Defense (FTD)
- Configuration IP SLA sur Cisco Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Device Manager (FDM)

Composants utilisés

Les informations contenues dans ce document sont basées sur la version logicielle et matérielle suivante :

- Cisco FTD version 7.4.1 (build 172)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit comment configurer Equal-Cost Multi-Path (ECMP) avec le protocole IP SLA (Internet Protocol Service Level Agreement) sur un FTD Cisco géré par Cisco FDM. ECMP vous permet de regrouper des interfaces sur FTD et d'équilibrer la charge du trafic sur plusieurs interfaces. IP SLA est un mécanisme qui surveille la connectivité de bout en bout par l'échange de paquets réguliers. Parallèlement à ECMP, IP SLA peut être mis en oeuvre afin de garantir la disponibilité du tronçon suivant. Dans cet exemple, le protocole ECMP est utilisé pour distribuer les paquets de manière égale sur deux circuits de fournisseur d'accès Internet (FAI).

Parallèlement, un IP SLA assure le suivi de la connectivité, assurant une transition transparente vers tous les circuits disponibles en cas de panne.

Les exigences spécifiques de ce document sont les suivantes :

- Accès aux périphériques avec un compte utilisateur avec des privilèges d'administrateur
- Cisco Secure Firewall Threat Defense version 7.1 ou ultérieure

Configurer

Diagramme du réseau

Dans cet exemple, Cisco FTD possède deux interfaces externes : outside1 et outside2 . Chacun se connecte à une passerelle ISP, outside1 et outside2 appartiennent à la même zone ECMP nommée outside.

Le trafic provenant du réseau interne est acheminé via FTD et la charge est équilibrée sur Internet via les deux FAI.

Dans le même temps, FTD utilise des SLA IP afin de surveiller la connectivité à chaque passerelle ISP. En cas de défaillance sur l'un des circuits du FAI, le FTD bascule vers l'autre passerelle du FAI pour assurer la continuité des activités.

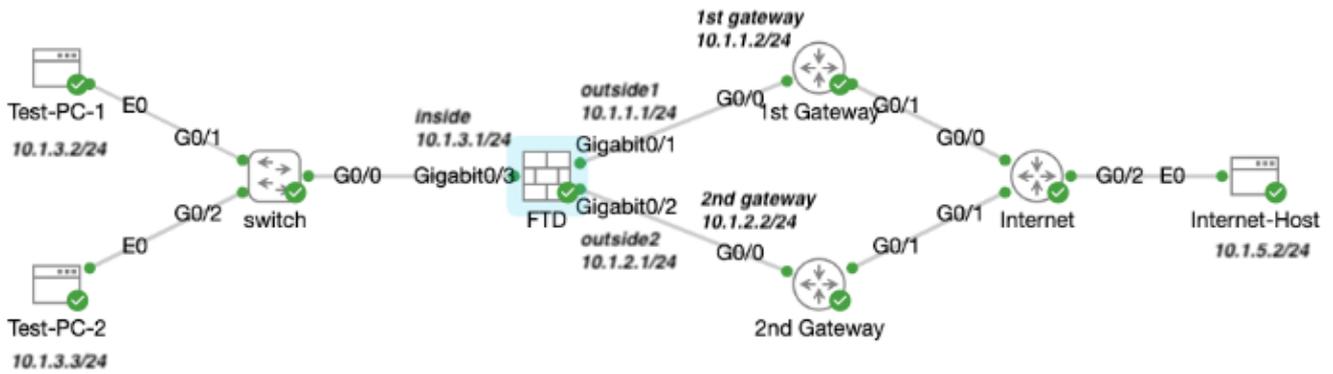
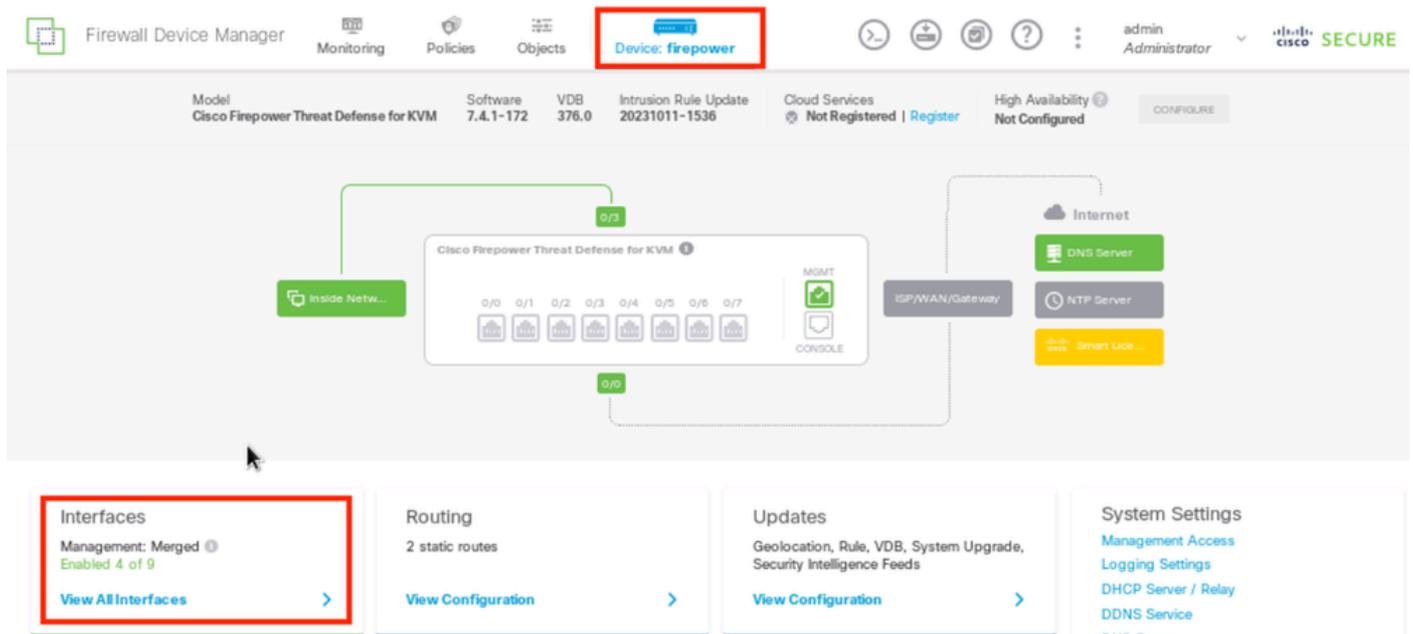


Diagramme du réseau

Configurations

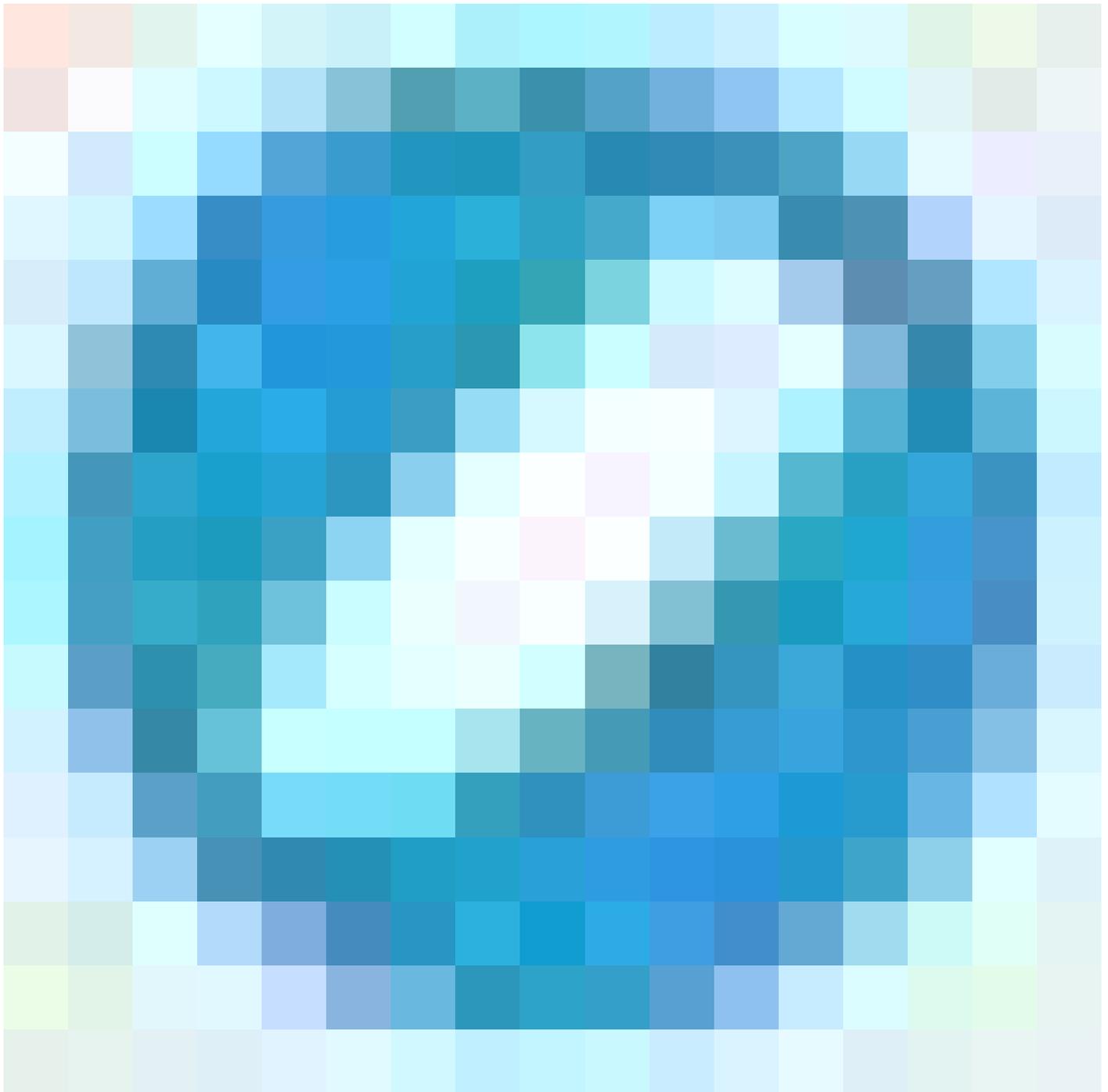
Étape 0. Préconfigurer les interfaces/objets

Connectez-vous à l'interface utilisateur graphique Web de FDM, cliquez sur Device , puis cliquez sur le lien dans le résumé Interfaces. La liste Interfaces affiche les interfaces disponibles, leurs noms, adresses et états.



Interface de périphérique FDM

Cliquez sur l'icône de modification (



) de l'interface physique que vous souhaitez modifier. Dans cet exemple, GigabitEthernet0/1.

Firewall Device Manager

Monitoring Policies Objects Device: firepower

admin Administrator

Device Summary

Interfaces

Cisco Firepower Threat Defense for KVM

0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7

MGMT

CONSOLE

Interfaces Virtual Tunnel Interfaces

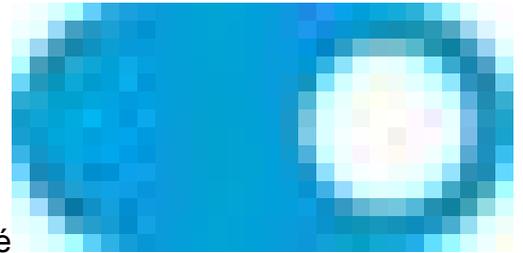
9 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STAND BY ADDRESS	MONITOR FOR HA	ACTIONS
> GigabitEthernet0/0	outside	<input type="checkbox"/>	Routed			Enabled	
> GigabitEthernet0/1	outside 1	<input checked="" type="checkbox"/>	Routed	10.1.1.1		Enabled	

Étape 0 Interface Gi0/1

Dans la fenêtre Modifier l'interface physique :

1. Définissez le nom de l'interface, dans ce cas en dehors de 1 .



2. Réglez le curseur Status sur le paramètre enabled (activé).
3. Cliquez sur l'onglet IPv4 Address et configurez l'adresse IPv4, dans ce cas 10.1.1.1/24.
4. Click OK.

GigabitEthernet0/1

Edit Physical Interface



Interface Name

outside1

Mode

Routed

Status



Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

10.1.1.1

/

255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

/

e.g. 192.168.5.16

CANCEL

OK

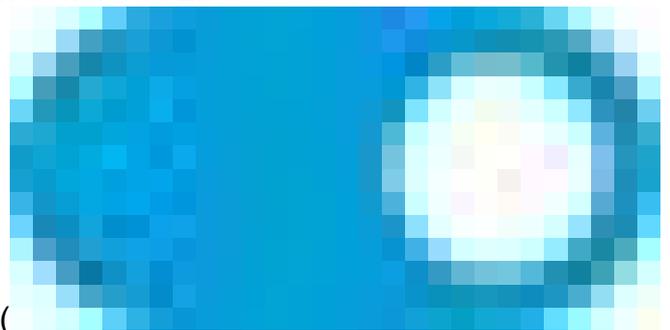
Étape 0 - Modifiez l'interface Gi0/1



Remarque : seules les interfaces routées peuvent être associées à une zone ECMP.

Répétez les étapes similaires pour configurer l'interface pour la connexion du FAI secondaire. Dans cet exemple, l'interface physique est GigabitEthernet0/2. Dans la fenêtre Modifier l'interface physique :

1. Définissez le nom de l'interface, dans ce cas en dehors de 2.



2. Réglez le curseur État sur le paramètre activé ().
3. Cliquez sur l'onglet IPv4 Address et configurez l'adresse IPv4, dans ce cas 10.1.2.1/24.

4. Click OK.

GigabitEthernet0/2
Edit Physical Interface

Interface Name:

Mode:

Status:

Description:

IPv4 Address | IPv6 Address | Advanced

Type:

IP Address and Subnet Mask: /

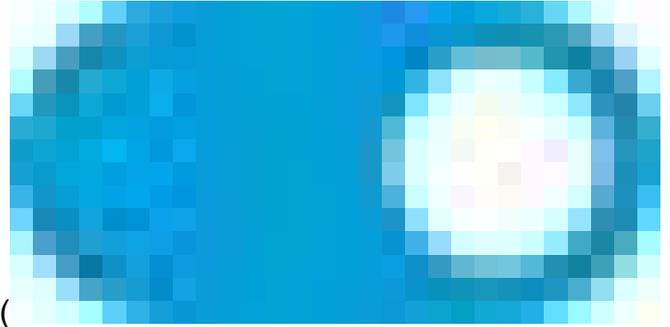
Standby IP Address and Subnet Mask: /

CANCEL OK

Étape 0 - Modifiez l'interface Gi0/2

Répétez les étapes similaires pour configurer l'interface pour la connexion interne, dans cet exemple, l'interface physique est GigabitEthernet0/3. Dans la fenêtre Modifier l'interface physique :

1. Définissez le nom de l'interface, dans ce cas à l'intérieur .



2. Réglez le curseur État sur le paramètre activé ().
3. Cliquez sur l'onglet IPv4 Address et configurez l'adresse IPv4, dans ce cas 10.1.3.1/24.
4. Click OK.

GigabitEthernet0/3

Edit Physical Interface

Interface Name:

Mode:

Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

IPv4 Address | IPv6 Address | Advanced

Type:

IP Address and Subnet Mask: /

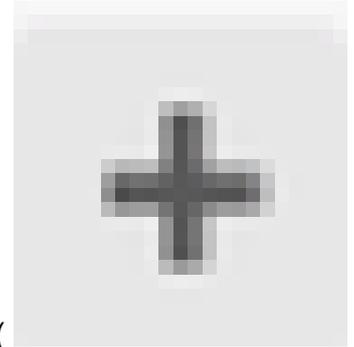
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask: /

e.g. 192.168.5.16

CANCEL OK

Étape 0 - Modifiez l'interface Gi0/3



Accédez à Objets > Types d'objets > Réseaux , cliquez sur l'icône d'ajout () pour ajouter un nouvel objet.

Firewall Device Manager

Monitoring Policies **Objects** Device: firepower

admin Administrator

Object Types

Networks

Ports

Security Zones

Application Filters

URLs

Geolocations

Syslog Servers

IKE Policies

Network Objects and Groups

8 objects

Filter

Preset filters: System-defined, User-defined

#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-All-RFC1918	Group	IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16	
2	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	
3	IPv4-Private-172.16.0.0-12	NETWORK	172.16.0.0/12	
4	IPv4-Private-192.168.0.0-16	NETWORK	192.168.0.0/16	
5	any-ipv4	NETWORK	0.0.0.0/0	
6	any-ipv6	NETWORK	::/0	

Étape 0 Objet 1

Dans la fenêtre Add Network Object, configurez la première passerelle ISP :

1. Définissez le Nom de l'objet, dans ce cas gw-outside1.
2. Sélectionnez le Type de l'objet, dans ce cas Hôte.
3. Définissez l'adresse IP de l'hôte, dans ce cas 10.1.1.2.
4. Click OK.

Add Network Object



Name

gw-outside1

Description

Type



Network



Host



FQDN



Range

Host

10.1.1.2

e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A

CANCEL

OK

Étape 0, objet 2

Répétez les étapes similaires pour configurer un autre objet réseau pour la deuxième passerelle ISP :

1. Définissez le Nom de l'objet, dans ce cas gw-outside2.
2. Sélectionnez le Type de l'objet, dans ce cas Hôte.
3. Définissez l'adresse IP de l'hôte, dans ce cas 10.1.2.2.
4. Click OK.

Add Network Object



Name

gw-outside2

Description

A large, empty text area for entering a description, with a small diagonal icon in the bottom right corner.

Type



Network



Host



FQDN



Range

Host

10.1.2|2

e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A

CANCEL

OK



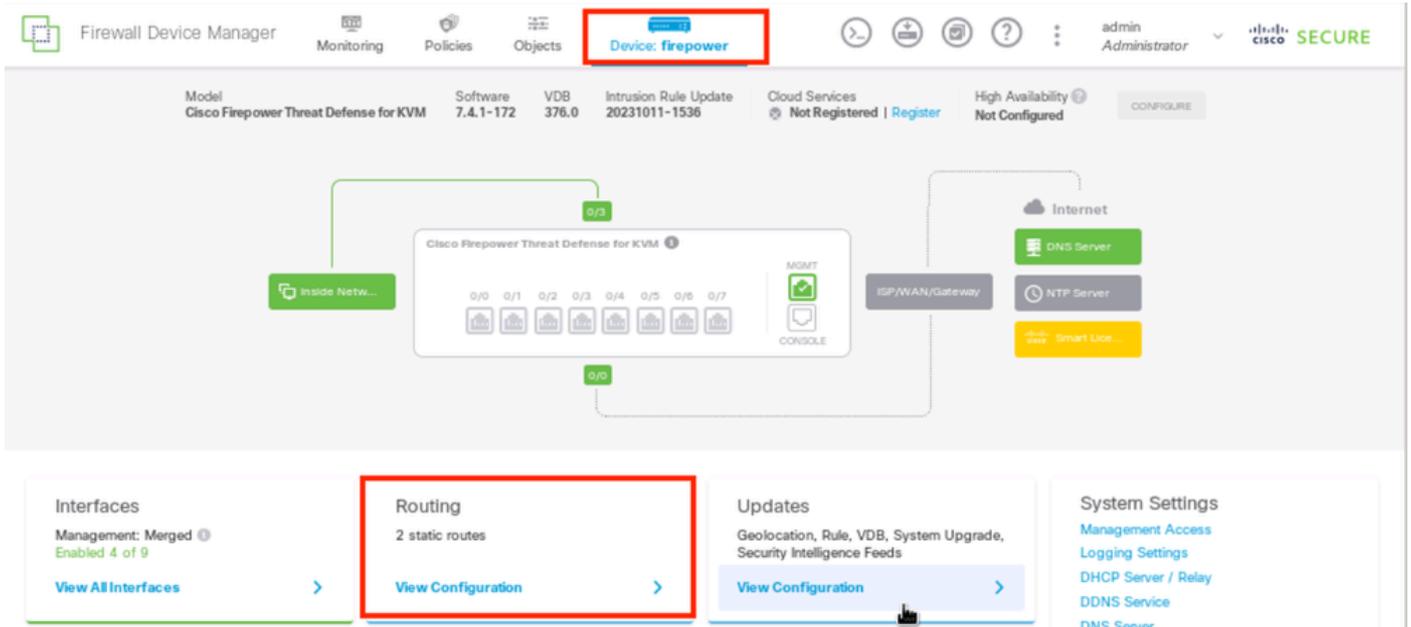
Remarque : votre stratégie de contrôle d'accès doit être configurée sur FTD pour autoriser le trafic. Cette partie n'est pas incluse dans ce document.

Étape 1. Configuration de la zone ECMP

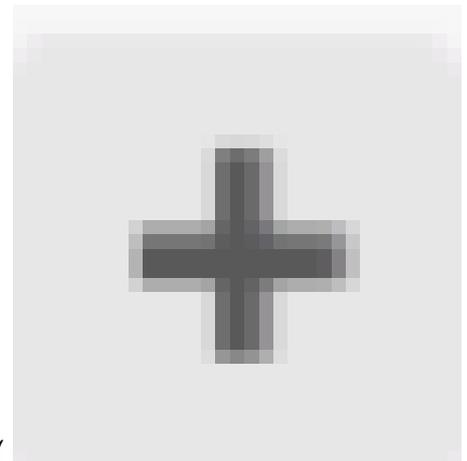
Accédez à [Device](#) , puis cliquez sur le lien dans le résumé du routage.



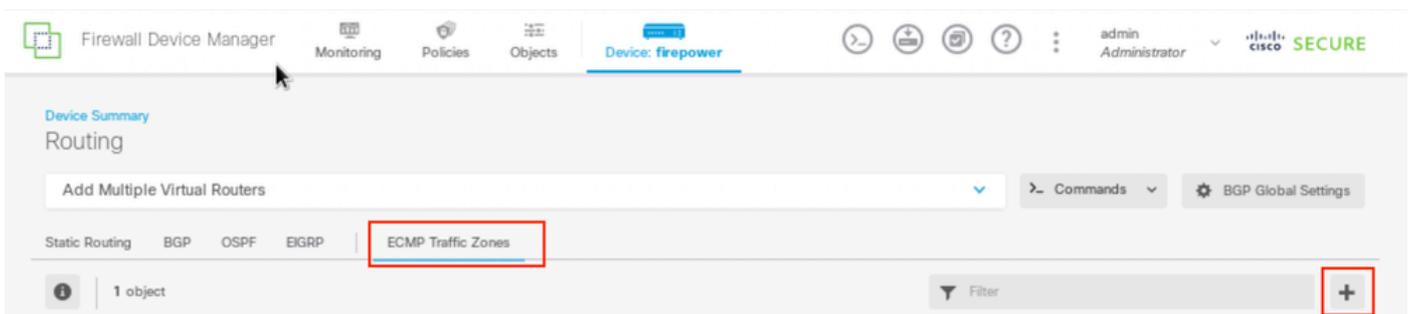
Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage () du routeur dans lequel vous configurez une route statique. Dans ce cas, les routeurs virtuels ne sont pas activés.



Étape 1 - ECMP Zone1



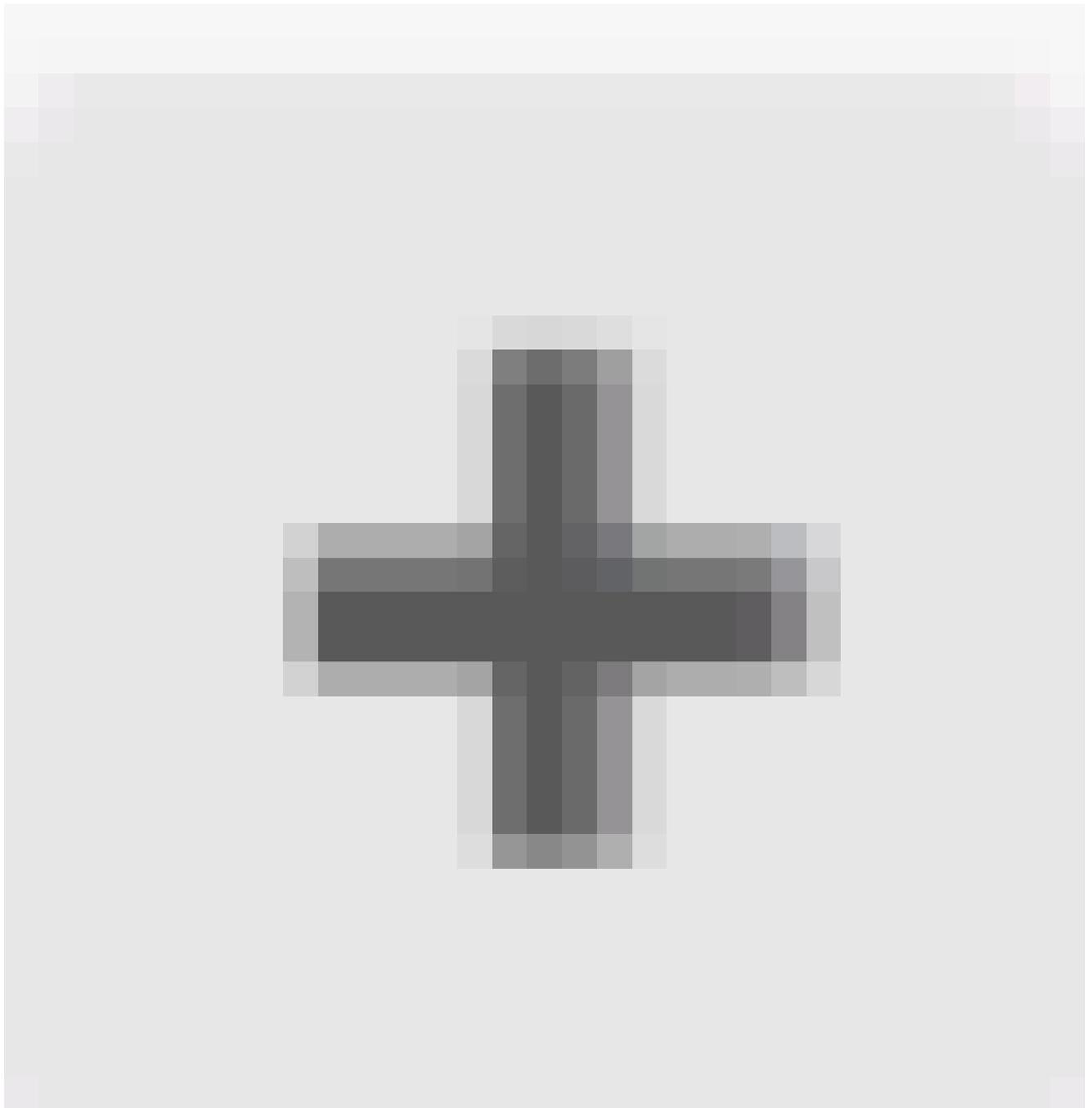
Cliquez sur l'onglet Zones de trafic ECMP, puis sur l'icône d'ajout () pour ajouter une nouvelle zone.



Étape 1 - ECMP Zone2

Dans la fenêtre Add ECMP Traffic Zone :

1. Définissez le nom de la zone ECMP et éventuellement une description.
2. Cliquez sur l'icône d'ajout ()



) pour sélectionner jusqu'à 8 interfaces à inclure dans la zone. Dans cet exemple, le nom ECMP est Outside, les interfaces outside1 et outside2 sont ajoutées à la zone.

3. Click OK.

Add ECMP Traffic Zone



i Keep the member interfaces of a ECMP traffic zone in the same security zone to prevent different access rules being applied to those interfaces.

Name

Outside

Description

Interfaces



- > inside (GigabitEthernet0/3)
- > management (Management0/0)
- > outside (GigabitEthernet0/0)
- > outside1 (GigabitEthernet0/1)
- > outside2 (GigabitEthernet0/2)

2 item(s) selected

Create new Subinterface

CANCEL

OK

CANCEL

OK

ADD ECMP TRAFFIC ZONE

Étape 1 - ECMP Zone3

Les deux interfaces outside1 et outside2 ont été ajoutées avec succès à la zone ECMP externe.

Device Summary
Routing

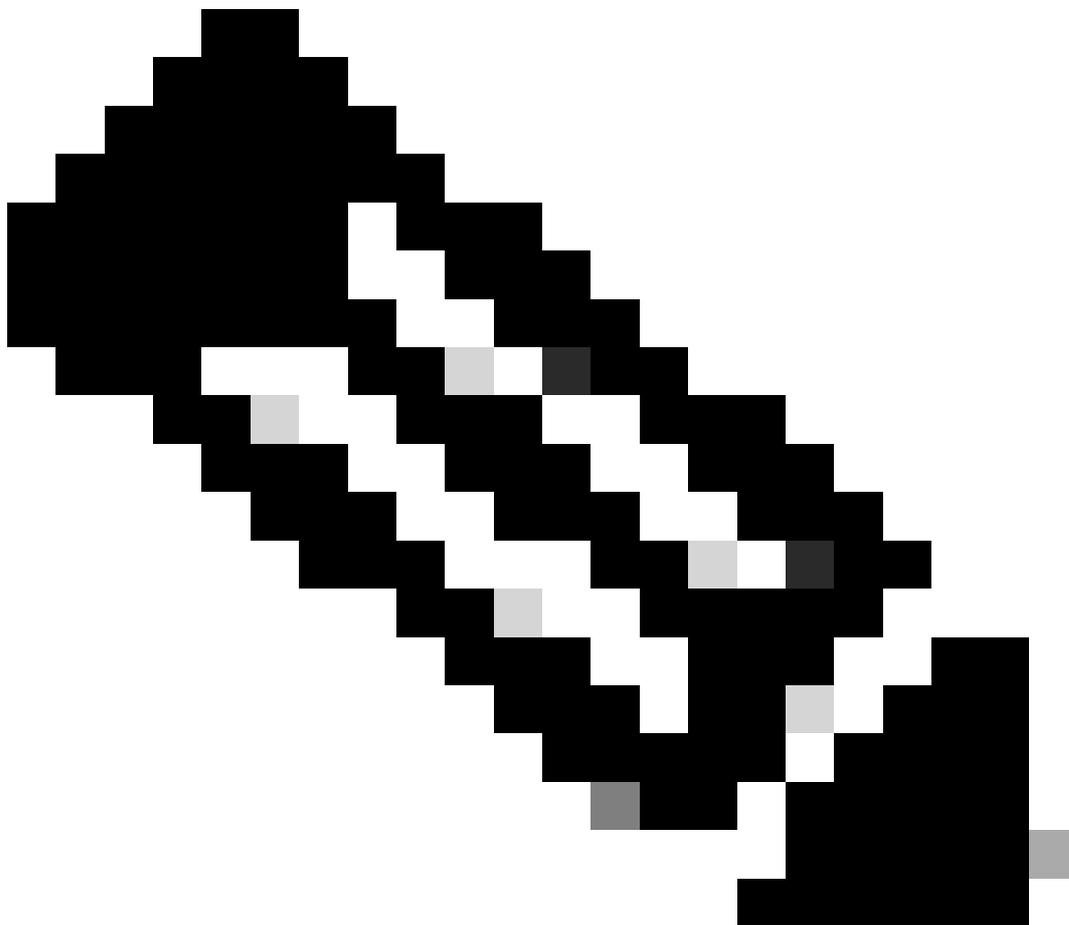
Add Multiple Virtual Routers ▼ Commands BGP Global Settings

Static Routing | BGP | OSPF | EIGRP | **ECMP Traffic Zones**

1 object Filter +

#	NAME	INTERFACES	ACTIONS
1	Outside	outside1 (GigabitEthernet0/1) outside2 (GigabitEthernet0/2)	

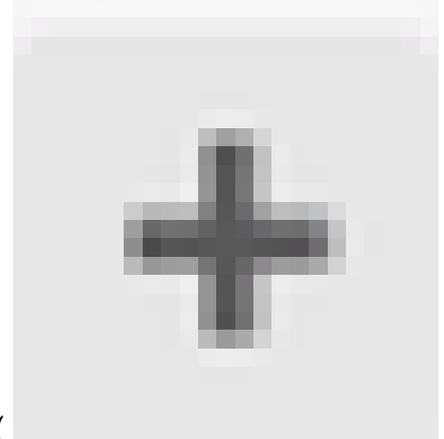
Étape 1 - ECMP Zone4



Remarque : une zone de trafic de routage ECMP n'est pas liée aux zones de sécurité. La création d'une zone de sécurité contenant les interfaces outside1 et outside2 n'implémente pas de zone de trafic pour le routage ECMP.

Étape 2. Configurer des objets IP SLA

Pour définir les objets SLA utilisés pour surveiller la connectivité à chaque passerelle, accédez à



Objets > Types d'objet > Moniteurs SLA , cliquez sur l'icône d'ajout () pour ajouter un nouveau moniteur SLA pour la première connexion ISP.

Étape2 IP SLA1

Dans la fenêtre Ajouter un objet SLA Monitor :

1. Définissez le Nom pour l'objet de surveillance SLA et éventuellement une description, dans ce cas sla-outside1.
2. Définissez l'adresse de surveillance, dans ce cas gw-outside1 (la première passerelle ISP).
3. Définissez l'interface cible par l'intermédiaire de laquelle l'adresse de surveillance est accessible, en l'occurrence en dehors de 1 .
4. En outre, il est également possible d'ajuster le délai d'attente et le seuil . Click OK.

Add SLA Monitor Object



Name

sla-outside1

Description

Monitor Address

gw-outside1

Target Interface

outside1 (GigabitEthernet0/1)

IP ICMP ECHO OPTIONS

i Following properties have following correlation: Threshold \leq Timeout \leq Frequency

Threshold

5000

milliseconds

0 - 2147483647

Timeout

5000

milliseconds

0 - 604800000

Frequency

60000

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28

0 - 16384

bytes

CANCEL

OK

Répétez l'étape similaire pour configurer un autre objet SLA Monitor pour la deuxième connexion ISP, dans la fenêtre Add SLA Monitor Object :

1. Définissez le Nom pour l'objet de surveillance SLA et éventuellement une description, dans ce cas sla-outside2 .
2. Définissez l'adresse de surveillance, dans ce cas gw-outside2 (la deuxième passerelle FAI).
3. Définissez l'interface cible par l'intermédiaire de laquelle l'adresse de surveillance est accessible, en l'occurrence en dehors de la zone 2.
4. En outre, il est également possible d'ajuster le délai d'attente et le seuil. Click OK.

Add SLA Monitor Object



Name

sla-outside2

Description

Monitor Address

gw-outside2

Target Interface

outside2 (GigabitEthernet0/2)

IP ICMP ECHO OPTIONS



Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

5000

milliseconds

0 - 2147483647

Timeout

5000

milliseconds

0 - 604800000

Frequency

60000

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28

0 - 16384

bytes

CANCEL

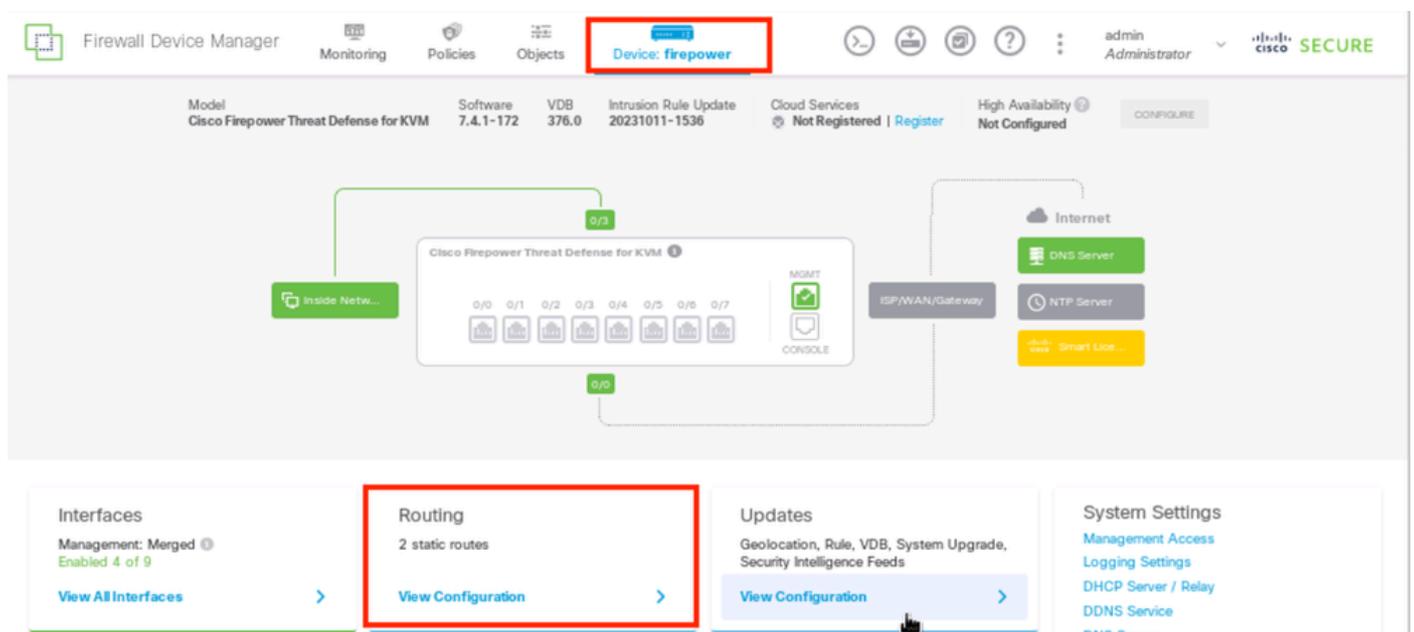
OK

Étape 3. Configuration de routes statiques avec route track

Accédez à Device , puis cliquez sur le lien dans le résumé du routage.

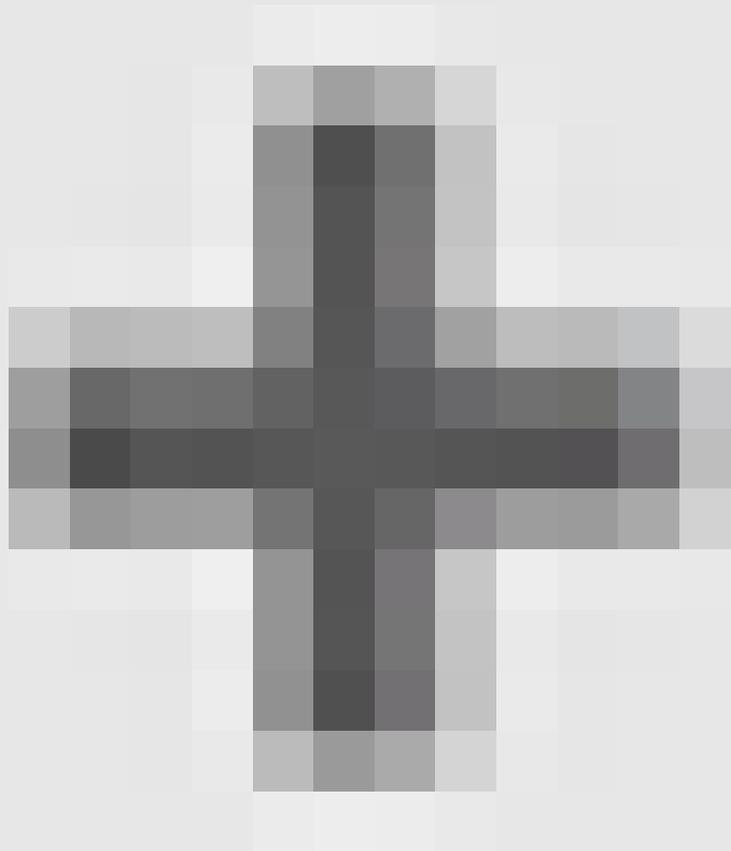


Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage () du routeur dans lequel vous configurez une route statique. Dans ce cas, les routeurs virtuels ne sont pas activés.



Étape 3 Route 1

Sur la page Static Routing, cliquez sur l'icône d'ajout (



) pour ajouter une nouvelle route statique pour la première liaison ISP.

Dans la fenêtre Ajouter une route statique :

1. Définissez le nom de la route et éventuellement la description. Dans ce cas, route_outside1.
2. Dans la liste déroulante Interface, sélectionnez l'interface par laquelle vous souhaitez envoyer le trafic, l'adresse de passerelle doit être accessible via l'interface. Dans ce cas, outside1 (GigabitEthernet0/1).
3. Sélectionnez les Réseaux qui identifient les réseaux de destination ou les hôtes qui utilisent la passerelle dans cette route. Dans ce cas, l'any-ipv4 prédéfini.
4. Dans la liste déroulante Gateway, sélectionnez l'objet réseau qui identifie l'adresse IP de la passerelle, Traffic is sent to this address. Dans ce cas gw-outside1 (la première passerelle

ISP).

5. Définissez la métrique de la route, entre 1 et 254. Dans cet exemple 1.
6. Dans la liste déroulante SLA Monitor, sélectionnez l'objet SLA Monitor. Dans ce cas, sla-outside1.
7. Click OK.

Add Static Route



Name

route_outside1

Description

Interface

outside1 (GigabitEthernet0/1)

Protocol

IPv4 IPv6

Networks



any-ipv4

Gateway

gw-outside1

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside1

CANCEL

OK

Répétez l'étape similaire pour configurer une autre route statique pour la deuxième connexion ISP, dans la fenêtre Add Static Route :

1. Définissez le nom de la route et éventuellement la description. Dans ce cas, route_outside2.
2. Dans la liste déroulante Interface, sélectionnez l'interface par laquelle vous souhaitez envoyer le trafic, l'adresse de passerelle doit être accessible via l'interface. Dans ce cas, outside2 (GigabitEthernet0/2).
3. Sélectionnez les Réseaux qui identifient les réseaux de destination ou les hôtes qui utilisent la passerelle dans cette route. Dans ce cas, l'any-ipv4 prédéfini.
4. Dans la liste déroulante Gateway, sélectionnez l'objet réseau qui identifie l'adresse IP de la passerelle, Traffic is sent to this address. Dans ce cas, gw-outside2 (la deuxième passerelle ISP).
5. Définissez la métrique de la route, entre 1 et 254. Dans cet exemple 1.
6. Dans la liste déroulante SLA Monitor, sélectionnez l'objet SLA Monitor. Dans ce scénario, sla-outside2.
7. Click OK.

Add Static Route



Name

route_outside2

Description

Interface

outside2 (GigabitEthernet0/2)

Protocol

IPv4 IPv6

Networks



any-ipv4

Gateway

gw-outside2

Metric

1

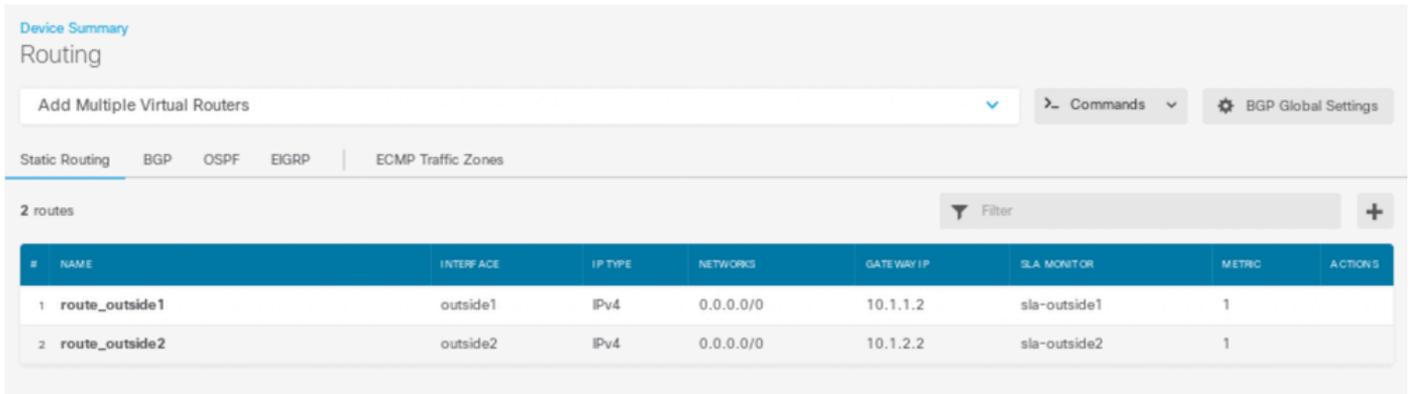
SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

Vous avez 2 routes via les interfaces outside1 et outside2 avec des pistes de route.



The screenshot shows the Cisco FTD Routing configuration page. At the top, there is a 'Device Summary' header and a 'Routing' section. Below this, there are tabs for 'Static Routing', 'BGP', 'OSPF', 'EIGRP', and 'ECMP Traffic Zones'. The 'Static Routing' tab is selected. A table displays two routes:

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	route_outside1	outside1	IPv4	0.0.0.0/0	10.1.1.2	sla-outside1	1	
2	route_outside2	outside2	IPv4	0.0.0.0/0	10.1.2.2	sla-outside2	1	

Étape 3 Route 4

Déployez la modification sur FTD.

Vérifier

Connectez-vous à l'interface de ligne de commande du FTD, exécutez la commande `show zone` pour vérifier les informations sur les zones de trafic ECMP, y compris les interfaces qui font partie de chaque zone.

```
<#root>
```

```
> show zone
```

```
Zone:
```

```
Outside
```

```
ecmp
```

```
Security-level: 0
```

```
Zone member(s): 2
```

```
outside2 GigabitEthernet0/2
```

```
outside1 GigabitEthernet0/1
```

Exécutez la commande `show running-config route` pour vérifier la configuration en cours de la configuration de routage. Dans ce cas, il existe deux routes statiques avec des routes.

```
<#root>
```

```
> show running-config route
```

```
route outside1 0.0.0.0 0.0.0.0 10.1.1.2 1 track 1
```

```
route outside2 0.0.0.0 0.0.0.0 10.1.2.2 1 track 2
```

Exécutez la commande `show route` pour vérifier la table de routage, dans ce cas, il y a deux routes par défaut sont via l'interface `outside1` et `outside2` à coût égal, le trafic peut être distribué entre deux circuits ISP.

```
<#root>
```

```
> show route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2
```

```
[1/0] via 10.1.1.2, outside1
```

```
C 10.1.1.0 255.255.255.0 is directly connected, outside1  
L 10.1.1.1 255.255.255.255 is directly connected, outside1  
C 10.1.2.0 255.255.255.0 is directly connected, outside2  
L 10.1.2.1 255.255.255.255 is directly connected, outside2  
C 10.1.3.0 255.255.255.0 is directly connected, inside  
L 10.1.3.1 255.255.255.255 is directly connected, inside
```

Exécutez la commande `show sla monitor configuration` pour vérifier la configuration du moniteur SLA.

```
<#root>
```

```
> show sla monitor configuration  
SA Agent, Infrastructure Engine-II  
Entry number: 1037119999  
Owner:  
Tag:
```

```
Type of operation to perform: echo
```

```
Target address: 10.1.1.2
```

```
Interface: outside1
```

Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 1631063762
Owner:
Tag:

Type of operation to perform: echo

Target address: 10.1.2.2

Interface: outside2

Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Exécutez la commande `show sla monitor operational-state` pour confirmer l'état du SLA Monitor. Dans ce cas, vous pouvez trouver « Timeout were: FALSE » dans le résultat de la commande, il indique que l'écho ICMP à la passerelle répond, de sorte que la route par défaut via l'interface cible est active et installée dans la table de routage.

<#root>

```
> show sla monitor operational-state
Entry number: 1037119999
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 79
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
```

Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE

Latest RTT (milliseconds): 1

Latest operation start time: 05:32:32.791 UTC Tue Jan 30 2024

Latest operation return code: OK

RTT Values:

RTTAvg: 1 RTTMin: 1 RTTMax: 1

NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 1631063762

Modification time: 04:14:32.771 UTC Tue Jan 30 2024

Number of Octets Used by this Entry: 2056

Number of operations attempted: 79

Number of operations skipped: 0

Current seconds left in Life: Forever

Operational state of entry: Active

Last time this entry was reset: Never

Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE

Latest RTT (milliseconds): 1

Latest operation start time: 05:32:32.791 UTC Tue Jan 30 2024

Latest operation return code: OK

RTT Values:

RTTAvg: 1 RTTMin: 1 RTTMax: 1

NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Équilibrage de charge

Traffic initial via FTD pour vérifier si la charge ECMP équilibre le trafic entre les passerelles de la zone ECMP. Dans ce cas, lancez la connexion SSH de Test-PC-1 (10.1.3.2) et Test-PC-2 (10.1.3.4) vers Internet-Host (10.1.5.2), exécutez la commande `show conn` pour confirmer que le trafic est équilibré en charge entre deux liaisons ISP, Test-PC-1 (10.1.3.2) passe par l'interface outside1, Test-PC-2 (10.1.3.4) passe par l'interface outside2.

<#root>

> show conn

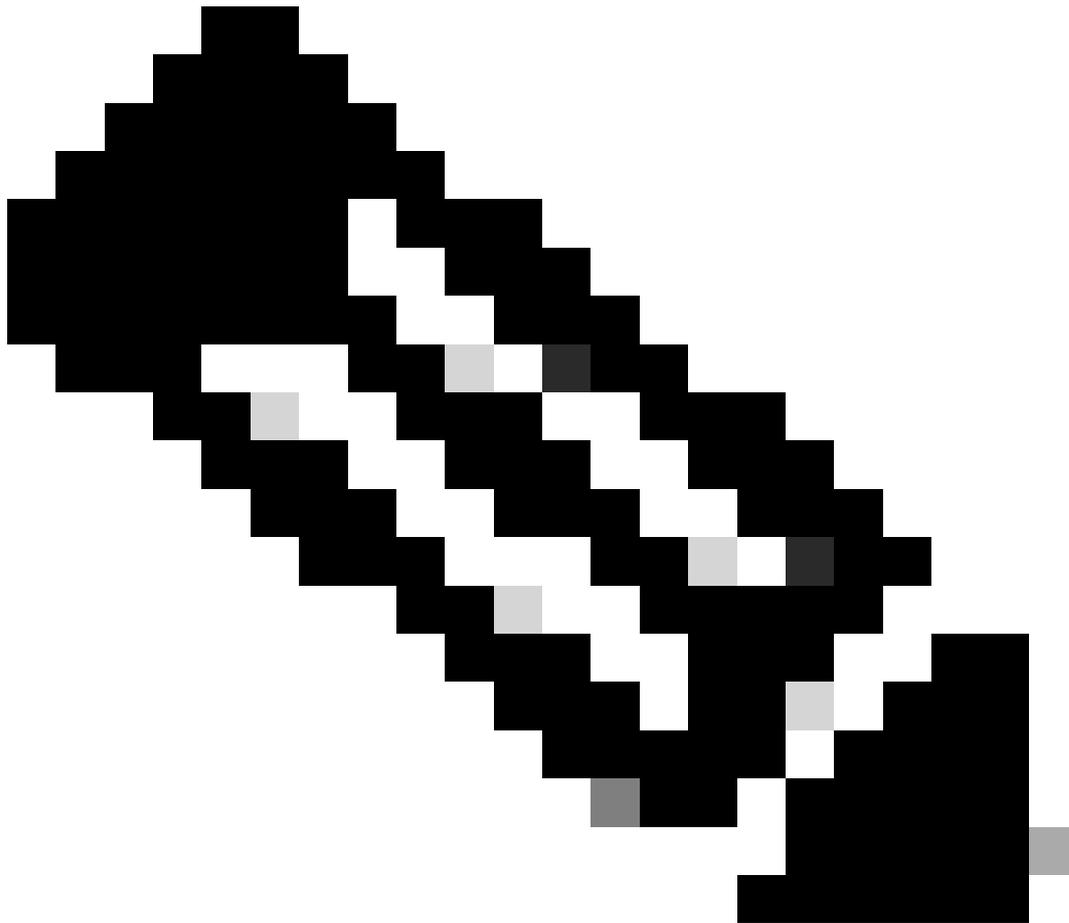
4 in use, 14 most used

Inspect Snort:

preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect

TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:02:10, bytes 5276, flags UIO N1

TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:00:04, bytes 5276, flags UIO N1



Remarque : la charge du trafic est répartie entre les passerelles spécifiées en fonction d'un algorithme qui hache les adresses IP source et de destination, l'interface entrante, le protocole, la source et les ports de destination. Lorsque vous exécutez le test, le trafic que vous simulez peut être routé vers la même passerelle en raison de l'algorithme de hachage, ce qui est attendu, changez n'importe quelle valeur parmi les 6 tuples (IP source, IP de destination, interface entrante, protocole, port source, port de destination) pour apporter des modifications au résultat du hachage.

Route perdue

Si la liaison vers la première passerelle ISP est désactivée, dans ce cas, arrêtez le premier routeur de passerelle pour simuler. Si le FTD ne reçoit pas de réponse d'écho de la première passerelle du FAI dans le délai spécifié dans l'objet SLA Monitor, l'hôte est considéré comme inaccessible et marqué comme inactif. La route suivie vers la première passerelle est également supprimée de la table de routage.

Exécutez la commande `show sla monitor operational-state` pour confirmer l'état actuel du SLA Monitor. Dans ce cas, vous pouvez trouver «

Timeout were: True » dans le résultat de la commande, il indique que l'écho ICMP à la première passerelle ISP ne répond pas.

<#root>

```
> show sla monitor operational-state
Entry number: 1037119999
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 121
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
```

Timeout occurred: TRUE

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 06:14:32.801 UTC Tue Jan 30 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0
```

```
Entry number: 1631063762
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 121
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
```

Timeout occurred: FALSE

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 06:14:32.802 UTC Tue Jan 30 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

Exécutez la commande **show route** pour vérifier la table de routage actuelle, la route vers la première passerelle ISP via l'interface outside1 est supprimée, il n'y a qu'une seule route active par défaut vers la deuxième passerelle ISP via l'interface outside2.

<#root>

```
> show route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2
```

```
C 10.1.1.0 255.255.255.0 is directly connected, outside1  
L 10.1.1.1 255.255.255.255 is directly connected, outside1  
C 10.1.2.0 255.255.255.0 is directly connected, outside2  
L 10.1.2.1 255.255.255.255 is directly connected, outside2  
C 10.1.3.0 255.255.255.0 is directly connected, inside  
L 10.1.3.1 255.255.255.255 is directly connected, inside
```

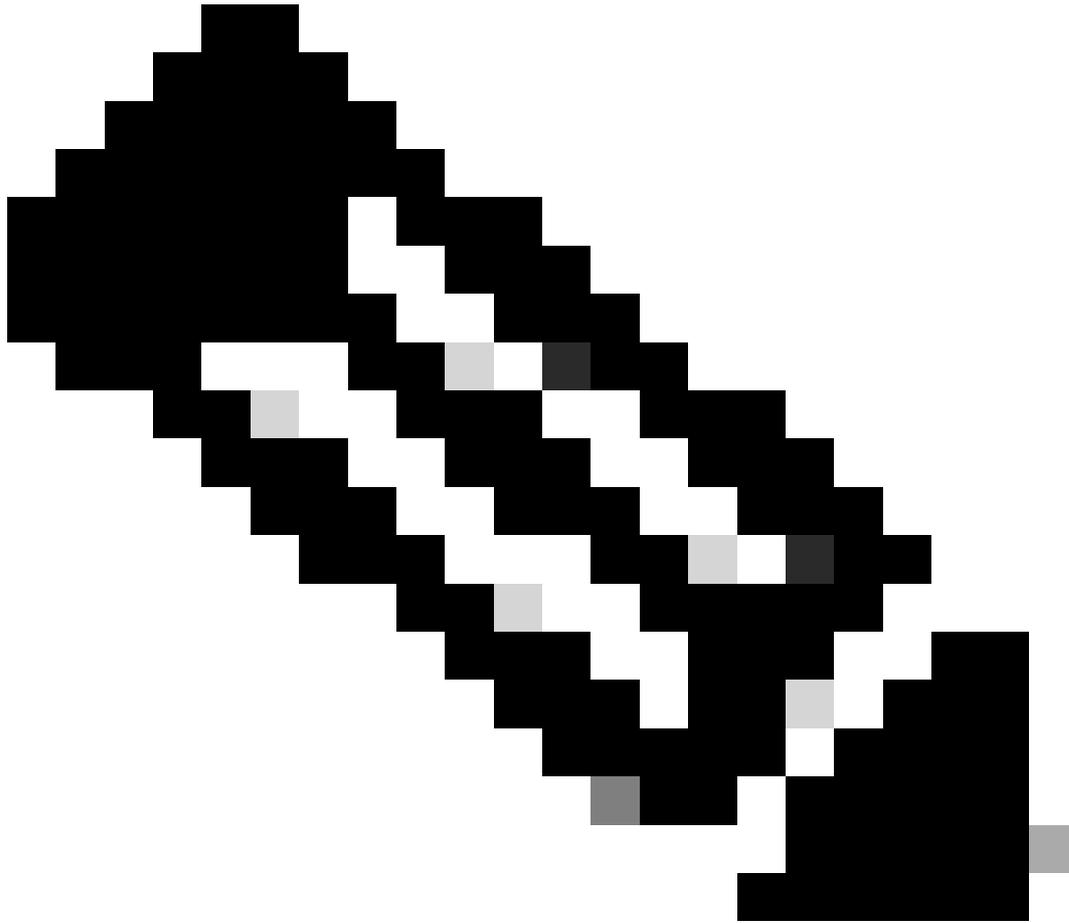
Exécutez la commande `show conn`, vous pouvez constater que les deux connexions sont toujours actives. Les sessions SSH sont également actives sur Test-PC-1 (10.1.3.2) et Test-PC-2 (10.1.3.4) sans interruption.

```
<#root>
```

```
> show conn  
4 in use, 14 most used  
Inspect Snort:  
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect
```

```
TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:19:29, bytes 5276, flags UIO N1
```

```
TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:17:22, bytes 5276, flags UIO N1
```



Remarque : vous pouvez remarquer dans le résultat de `show conn` , que la session SSH de Test-PC-1 (10.1.3.2) passe toujours par l'interface `outside1`, bien que la route par défaut via l'interface `outside1` ait été supprimée de la table de routage. ceci est attendu et, par conception, le trafic réel passe par l'interface `outside2`. Si vous initiez une nouvelle connexion de Test-PC-1 (10.1.3.2) à Internet-Host (10.1.5.2), vous pouvez constater que tout le trafic passe par l'interface `outside2`.

Dépannage

Afin de valider la modification de la table de routage, exécutez la commande `debug ip routing` .

Dans cet exemple, lorsque la liaison vers la première passerelle ISP est désactivée, la route passant par l'interface `outside1` est supprimée de la table de routage.

<#root>

```
> debug ip routing
IP routing debugging is on
```

RT:

```
ip_route_delete 0.0.0.0 0.0.0.0 via 10.1.1.2, outside1
```

```
ha_cluster_synced 0 routetype 0
```

```
RT: del 0.0.0.0 via 10.1.1.2, static metric [1/0]NP-route: Delete-Output 0.0.0.0/0 hop_count:1 , via 0.0.0.0
```

RT(mgmt-only):

```
NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, outside2
```

```
NP-route: Update-Input 0.0.0.0/0 hop_count:1 Distance:1 Flags:0X0 , via 10.1.2.2, outside2
```

Exécutez la commande `show route` pour confirmer la table de routage actuelle.

<#root>

```
> show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2
```

```
C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside
```

Lorsque la liaison vers la première passerelle ISP est à nouveau active, la route passant par l'interface `outside1` est ajoutée à la table de routage.

<#root>

```
> debug ip routing
IP routing debugging is on
```

```
RT(mgmt-only):
```

```
NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, outside2
```

```
NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.1.2, outside2
```

```
NP-route: Update-Input 0.0.0.0/0 hop_count:2 Distance:1 Flags:0X0 , via 10.1.2.2, outside2
via 10.1.1.2, outside1
```

Exécutez la commande `show route` pour confirmer la table de routage actuelle.

```
> show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2
[1/0] via 10.1.1.2, outside1
C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside
```

Informations connexes

- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.